Sensible Daten im Gepäck

Die Zahl an Cybervorfällen und Datenmissbrauch nimmt zu. Und mit der ab Mai geltenden EU-Datenschutz-Grundverordnung wird die Rechtslage weiter verschärft. Welche Auswirkungen hat sie auf Entsendungen innerhalb der EU und worauf müssen Personaler achten?

▸ Immer mehr wirtschaftliche Schäden weltweit werden durch sogenannte Cybervorfälle verursacht. Dabei handelt es sich vereinfacht ausgedrückt um Angriffe in der digitalen Infrastruktur eines Unternehmens. Die Ziele können vielfältig sein – entweder sollen der Betriebsablauf gestört, Geschäftsgeheimnisse gestohlen oder Einsicht in personenbezogene Daten erhalten werden. Tatsächlich rangieren Cybergefährdungen laut dem aktuellen Allianz Risk Barometer derzeit auf Rang zwei der zehn wichtigsten globalen Geschäftsrisiken 2017. Zum Vergleich: Noch vor fünf Jahren lag dieses Risiko lediglich auf Platz 15. Die Besorgnis der Unternehmen nimmt auch deshalb zu, weil diese Art der Gefährdung größtenteils noch eine „Blackbox" darstellt und nicht auf eine bestimmte Branche oder Firmengröße begrenzt ist – sie kann im Grunde jeden treffen. Nach professionellen Hackerangriffen ist die Hauptursache für einen Cyberangriff in einer Firma eine Daten- oder Sicherheitsverletzung. Deshalb gewinnt der Schutz von Daten innerhalb von Betrieben und Institutionen eine rasant zunehmende Bedeutung.

Kernpunkte der DSGVO

Ein wichtiger Schritt in Richtung Cybersicherheit ist die neue EU-Datenschutz-Grundverordnung (DSGVO), die ab dem 25. Mai 2018 das Datenschutzrecht innerhalb der Europäischen Union (EU) vereinheitlichen, aber auch verschärfen soll. Diese EU-Verordnung Nr. 2016/679 ersetzt die Richtlinie Nr. 95/46/EG. Im Kern sorgt sie dafür, dass der Ort der Datenverarbeitung keine Rolle mehr spielt. Wer immer sein Angebot oder seine Dienstleistung an EU-Bürger richtet, muss sich dem europäischen Datenschutzrecht unterordnen – das gilt beispielsweise auch für Google und Facebook. Das Netzwerk hat vor Kurzem Negativschlagzeilen gemacht, weil es millionenfach private Daten von Nutzern an eine Analysefirma weitergegeben hat, die nun im Verdacht stehen, sowohl das Brexit-Referendum als auch die US-Wahl beeinflusst zu haben.

Des Weiteren besteht nun in allen Mitgliedstaaten für Arbeitnehmer das einheitliche Recht, zu erfahren, wofür Arbeitgeber ihre Daten verwenden und verarbeiten. Auch ein Recht darauf, diese wieder zu löschen beziehungsweise löschen zu lassen, wurde eingeräumt. Neu ist auch, dass Unternehmen eine Beweislastumkehr haben. Das bedeutet, dass sie jederzeit dokumentieren müssen, wie und wo Daten von beispielsweise Kunden, aber auch Mitarbeitern gespeichert werden, wie diese erhoben werden und wer alles darauf Zugriff hat. Die neue Verordnung sieht weiter vor, dass Datenschutzverstöße von Mitarbeitern oder anderen Beteiligten, unabhängig von deren Aufenthaltsort, künftig innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde gemeldet werden müssen. Internationale Firmen und Organisationen

melden Vorfälle dann nur noch an die für ihren Hauptsitz zuständige „federführende Aufsichtsbehörde".
Die Kommission hat darüber hinaus die Bußgelder bei Datenschutzverstößen drastisch erhöht. So können Strafen bis zu 20 Millionen Euro oder vier Prozent des gesamten global erzielten Jahresumsatzes betragen. Unter Umständen sind Beträge in schwindelerregender Höhe fällig. Damit ist Europa nicht allein, denn weltweit verschärfen die Regierungen ihre Datenschutzregelungen. Besonders strenge Gesetze gibt es bereits in den USA, im Nahen Osten, Australien und Singapur. In den Vereinigten Staaten betrug die höchste bisher gezahlte Strafe wegen Verletzung des Datenschutzes gegenüber einem Kunden satte 100 Millionen US-Dollar. In den arabischen Ländern drohen selbst bei geringen Verstößen schnell Haftstrafen.

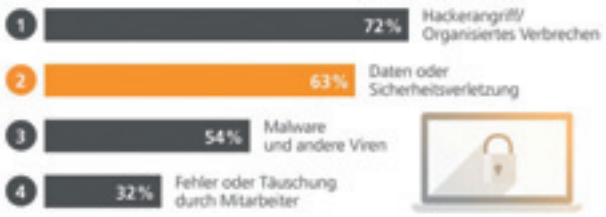
Folgen für die Entsendung ins Ausland

Was bedeutet dies für Unternehmen, die Mitarbeiter ins Ausland entsenden? Bei Entsendungen und Geschäftsreisen nach Europa bedeutet etwa die neue Datenschutzverordnung, dass Personalverantwortliche sich im Grunde mit den Datenschutzgesetzen aller EU-Länder auseinandersetzen müssen, in die sie Arbeitnehmer entsenden oder verleihen. Der Grund: Zwar gilt die neue Verordnung für alle EU-Mitgliedstaaten gleichermaßen – auch vollkommen unabhängig von der Unternehmensgröße –, aber wenn es um die Angestellten geht, so dürfen die Länder ihre eigenen Regeln über die nationalen Datenschutzgesetze vereinbaren. Dennoch ist es unwahrscheinlich, dass diese Regeln in den einzelnen Ländern signifikant voneinander abweichen werden. Denn laut der EU-Vorgabe dürfen sie zwar spezifisch, aber ihrem Wesen nach nicht unterschiedlich sein. Verantwortliche im Bereich Global Mobility sollten daher aus eigenem Interesse sowohl Geschäftsreisende als auch entsendete Mitarbeiter (Expats) über mögliche Sicherheitsrisiken und entsprechende Maßnahmen umfassend informieren. Idealerweise ist das Thema bereits in die Entsende- und Geschäftsreiserichtlinie integriert.

Neuerungen auch im deutschen Gesetz

In Deutschland gibt es seit Einführung der Datenschutz-Grundverordnung ein neues Bundesdatenschutzgesetz (BDSG-neu), aus dem auch ein neues Beschäftigtendatenschutzgesetz (Paragraf 26 BDSG-neu) resultiert. Zwar entspricht Paragraf 26 BDSG-neu im Wesentlichen dem bisherigen Paragraf 32 BSDG, allerdings gibt es noch einige klarstellende Regelungen. Diese betreffen etwa Tarifverträge und Dienstvereinbarungen, die für die Verarbeitung personenbezogener Daten herangezogen werden können. Die Vorgaben für den Beschäftigungsdatenschutz in Deutschland werden in Zukunft grundsätzlich durch Artikel 88 DSGVO in Verbindung mit Paragraf 26 BDSG-neu bestimmt.
Schickt also eine in der Bundesrepublik ansässige Firma einen Mitarbeiter ins Ausland, so muss sie sich an die genannten Vorgaben halten. Das gilt vor allem auch für die Frage, welche Mitarbeiterdaten an den Auftraggeber oder Entleiher im Ausland

Hauptursachen für Cybervorfälle in Firmen



Quelle: Allianz Risk Barometer 2017

Die größte Sicherheitsgefahr nach Hackerangriffen ist der Verlust von Daten, der gerade auch bei Geschäftsreisen vorkommen kann.

weitergegeben werden dürfen. Sitzt der Auftraggeber oder Entleiher allerdings nicht in der EU, kommen darüber hinaus noch die Artikel 44 ff. DSGVO ins Spiel. Das bedeutet also, dass der Auftraggeber oder Entleiher für den entsandten Mitarbeiter die Vorschriften der DSGVO anwenden muss und – sofern anwendbar – auch noch die konkretisierenden nationalen Vorschriften berücksichtigen sollte. Bei einem Auftraggeber oder Entleiher in einem Drittland käme dagegen das jeweilige lokale Datenschutzrecht zur Anwendung.
Wird umgekehrt ein Mitarbeiter aus dem Ausland nach Deutschland entsandt (Impat), gelten für das Arbeitsverhältnis zwischen diesem und dem Arbeitgeber im Entsendeland hinsichtlich des Beschäftigtendatenschutzes in der Regel die jeweiligen nationalen Bestimmungen, gegebenenfalls in Verbindung mit Artikel 88 DSGVO. Im Verhältnis zwischen dem Impat und dem Auftraggeber in Deutschland gelten im Hinblick auf den Datenschutz wiederum grundsätzlich die Bestimmungen der DSGVO. Solange kein Arbeitsverhältnis besteht, gelten grundsätzlich die allgemeinen datenschutzrechtlichen Bestimmungen und nicht die des Beschäftigtendatenschutzes. Sobald die Entsendung jedoch im Rahmen einer Arbeitnehmerüberlassung stattfindet, ist bislang umstritten, ob der Leiharbeitnehmer Beschäftigter im Sinne des Datenschutzrechtes ist. Wenn ja, wäre auch dort Artikel 88 DSGVO in Verbindung mit Paragraf 26 BDSG und damit Beschäftigtendatenschutzrecht anzuwenden. In der Praxis wird wahrscheinlich die Rechtsprechung hier Klarheit schaffen.

Risikofaktor Mensch

Unabhängig von den Vorkehrungen und Bemühungen international tätiger Unternehmen bereitet immer auch der „Faktor Mensch" Probleme. Zur Darstellung: Allein an den acht größten Flughäfen Europas verschwinden jährlich 175 000 Laptops mit wertvollen Daten. Mehr als der Verlust der Hardware wiegt jener der oftmals sensiblen Daten. Nicht erfasst in der Statistik sind etwa verloren gegangene USB-Sticks, Firmenhandys oder -tablets. Im Geschäftsalltag sollten Unternehmen deshalb mithilfe ihrer IT-Spezialisten und Datenschutzbeauftragen dafür sorgen, dass entsprechende praktische Vorkehrungen getroffen werden, die das Risiko für Datenverlust und für Cyber-Angriffe

minimieren. So ist es beispielsweise sinnvoll, die inzwischen miteinander vernetzten Geräte nicht nur durch entsprechende Programme zu schützen, sondern möglichst Verbindungen zu anderen firmeninternen PCs und technischen Anlagen vor einer Reise zu kappen.

Empfehlenswert ist es zudem, nur die nötigsten für die Entsendung oder Geschäftsreise relevanten Daten mitzuführen und zu speichern. Doch Vorsicht bei verschlüsselten Geräten und Daten: Viele Länder, und dazu gehören nicht nur autokratisch geführte Regimes, verlangen oft die Herausgabe von Passwörtern. In Frankreich und Großbritannien etwa dürfen die Behörden dies sogar per Gesetz. Wer sich bei einer Kontrolle am Flughafen weigert, das Passwort zu nennen, darf in Zwangshaft genommen werden.

Ein weiterer riesiger Unsicherheitsfaktor in puncto Datenschutz und -sicherheit sind Smartphone-Apps auf den mobilen Endgeräten der Mitarbeiter. Viele von diesen ermöglichen einen direkten Zugriff auf sensible Firmendaten beispielsweise auf dem Mobiltelefon. Laut dem Geschäftsreise-Verband VDR haben 65 Prozent der Unternehmen ihren Mitarbeitern keine entsprechenden Vorgaben zur Nutzung gemacht. Das ist überaus fahrlässig und bei Datensicherheitsverstößen werden die Unternehmen sehr wahrscheinlich zur Verantwortung gezogen werden.

Ein weiteres unterschätztes Risiko sind Führungskräfte auf Reisen. Nicht selten kommt es vor, dass diese beispielsweise in der Businesslounge am Flughafen lautstark Telefonate führen oder freie Sicht auf Firmeninterna auf ihrem Laptop oder Tablet bieten und somit Spionen geheime Daten wortwörtlich auf dem Silbertablett servieren. Hier gilt es, nicht nur im Vorfeld aufzuklären, sondern auch mögliche Sanktionen festzulegen.

Datenfalle Tracking-Tools

Ein anderes, nicht minder aktuelles datenschutzrechtliches Problem stellt sich insbesondere bei Auslandsentsendungen in Krisenregionen. Die Frage, wo der Mitarbeiter sich aktuell aufhält, ist Teil des Krisenmanagements in Unternehmen. So bieten immer mehr auf Travel Management spezialisierte Dienstleister spezielle Tracking-Tools an. Per Klick lässt sich mit dieser Software der Aufenthaltsort von Mitarbeitern ermitteln, um im Notfall sofort Hilfe zu organisieren. Geht dem Expat beispielsweise ein lebensnotwendiges Medikament aus, könnte sein Unternehmen dafür sorgen, dass der Dienstleister die Arznei binnen weniger Stunden zum Mitarbeiter vor Ort bringt.

Die Grundlage solcher Tracking-Systeme bilden die Reise- und Buchungsdaten der jeweiligen entsandten Mitarbeiter. Bei der Flugbuchung werden die sogenannten PNR-Daten (Passenger Name Record) über Schnittstellen aus diversen Buchungssystemen in die Tracking-Software eingespielt. Kommt es zu einer Krisensituation (zum Beispiel Terroranschläge, politische Unruhen oder Naturkatastrophen), prüft der Dienstleister binnen weniger Minuten, wo sich der Mitarbeiter im entsprechenden Moment aufhält und kann ihn evakuieren. Es ist jedoch fraglich, inwieweit dies mit den neuen Datenschutzregeln vereinbar ist, denn schlussendlich ist es ein Leichtes, auf Basis dieser Daten ein umfangreiches Persönlichkeitsprofil zu erstellen, von dem der Mitarbeiter nicht möchte, dass es in falsche Hände gelangt.

Besserer Datenschutz auf Auslandsreisen

- Nur die nötigsten Geräte und relevanten Datenträger mitnehmen, immer an dieselbe Stelle legen; Datenträger niemals unbeaufsichtigt lassen
- Back-up- und Sicherheitssoftware stets auf dem neuesten Stand halten
- Keine öffentlichen WLAN-Netzwerke, „Hotspots" zum Beispiel auf Flughäfen, nutzen (besser: UMTS-Sticks)
- Auf Reise-Apps verzichten
- Sichtschutzfolien auf Laptop oder Tablets benutzen
- Kameras auf Laptops, Tablets und Smartphones zukleben
- Daten verschlüsseln, aber Achtung: In vielen Ländern (beispielsweise USA, China, arabische Staaten) verlangt der Zoll, die Daten offenzulegen, sonst droht möglicherweise Einreiseverbot und sogar Beugehaft.
- Geheime Daten verstecken: zum Beispiel mithilfe diverser Programme Texte in einem Bild oder einer Grafik verschlüsseln
- Vernetzung mit anderen Datenträgern und PCs im Unternehmen kappen
- Zweitgeräte für Vielreisende anschaffen. Diese sind oft günstiger als spezielle Sicherheitsvorkehrungen und eine Vernetzung oder Synchronisation (zum Beispiel per VPN) muss nicht eingerichtet werden.

Der „gläserne" Mitarbeiter

Und noch ein weiteres, weitgehend unbekanntes und kaum thematisiertes Datenschutzproblem betrifft insbesondere Mitarbeiter von Unternehmen, die im Ausland zum Arzt gehen: Während Personaler für gewöhnlich niemals Einblick in die Gesundheitsakte ihrer in Deutschland verbleibenden Mitarbeiter erhalten könnten, wissen sie bei Expats und Auslandsreisenden unter Umständen und unfreiwillig ganz genau, unter welchen Krankheiten und Beschwerden diese leiden. Der Grund: Laut Paragraf 17 des fünften Sozialgesetzbuches (SGB V) bekommt der gesetzlich oder freiwillig in der GKV versicherte Arbeitnehmer – sowie dessen mitversicherte Angehörige – die Kosten, die während des Auslandsaufenthalts entstanden sind, durch den Arbeitgeber ersetzt. Um diese Gesundheitskosten jedoch erstattet zu bekommen, muss er die vom medizinischen Dienstleister überlassene Rechnung dem Arbeitgeber vorlegen, der somit genau Bescheid weiß, welche mitunter gravierenden oder unangenehmen gesundheitlichen Probleme den Mitarbeiter plagen. Eine datenschutzrechtliche Lösung hat der Gesetzgeber hier auch mit der DSGVO bislang nicht geschaffen, die Lücke bleibt bestehen. Um Konfliktpotenzial zu reduzieren, empfiehlt es sich, eine Restkostenversicherung abzuschließen, die den Erstattungsprozess mit den Kassen direkt vornimmt, ohne dass Travel Manager oder Personaler Einblick in die Rechnungen der Mitarbeiter im Ausland nehmen können. ■

AUTORIN

Anne-Katrin Schulz, Leiterin Unternehmenskommunikation und Marketing, BDAE Gruppe, Hamburg, akschulz@bdae.com